MAT 312 Spring 2009 Review for Final

FINAL IS CUMULATIVE: ALSO USE REVIEW SHEETS FOR MIDTERMS I AND II.

Final is "open book." You may consult Laufer, and you may use a TI-82 ... TI-86-class calculator. No computer algebra (no TI-89, for example). No cell phones.

9.1 Be able to use the Euclidean algorithm to calculate the greatest common divisor $g = (a, b)$ of two integers a and b. Also be able to run the algorithm backwards to find integers λ, μ such that $g = \lambda a + \mu b$. Examples 9.4, 9.5. Understand how to add and multiply equivalence classes *modulo* n ("mod n") as in Proposition 9.3. Understand Theorem 9.4: the equation $ax = 1$ in $\mathbf{Z}_n$ has a unique solution if and only if $(a, n) = 1$. Example 9.11. Note that this involves the λ, μ from the Euclidean Algorithm.

9.2 Understand the of definition of a *ring* and know the elementary examples $\mathbf{Z}, \mathbf{Z}_n$ (for any positive integer n) as well as $\mathbf{Q}, \mathbf{R}, \mathbf{C}$. Review arithmetic, absolute values, $re^{i\theta}$ notation for complex numbers. Understand that if R is a ring, the set $R[X]$ of polynomials with coefficients in R is also a ring, with the usual addition and multiplication of polynomials. (Definition on p. 430). Understand what it means for an element of a ring to be *invertible*. Understand the proof of Proposition 9.10. Be able to carry out "polynomial long division" in $R[X]$ when the divisor has invertible leading coefficient, and understand why that requirement is necessary in general; Theorem 9.11. Understand how $p \in R[X]$ determines a function $R \to R$ (definition on p. 436), but that for a general R, the polynomial is not determined by its values (Example 9.27). Understand the Remainder Theorem (Theorem 9.12) - this will be very important in section 9.3.

9.3 Have a good idea of how the Fourier series

$$f(x) \sim a_0 + \sum_{m=0}^{\infty} (a_m \cos mx + b_m \sin mx)$$

is calculated for a real-valued function defined on $[0, 2\pi]$ or for a periodic function of period 2π (the function may have a finite number of jump-discontinuities in $[0, 2\pi]$). I.e.

$$a_0 = \frac{1}{2\pi} \int_0^{2\pi} f(x)\, dx, \qquad a_m = \frac{1}{\pi} \int_0^{2\pi} f(x) \cos mx\, dx, \qquad b_m = \frac{1}{\pi} \int_0^{2\pi} f(x) \sin mx\, dx.$$

Be able to calculate the Fourier series for $f(x) = 1 \quad (0 \le x < \pi)$ and $= -1 \quad (\pi \le x \le 2\pi)$, and other simple functions. Be comfortable with going back and forth between these Fourier series and the complex Fourier series

$$f(x) \sim \sum_{m=-\infty}^{\infty} c_m e^{-imx} :$$

$$a_0 = c_0 \text{ and } \begin{cases} a_m = c_m + c_{-m}, & b_m = i(-c_m + c_{-m}) \\ c_m = \frac{1}{2}(a_m + ib_m), & c_{-m} = \frac{1}{2}(a_m - ib_m) \end{cases} \quad \text{for } m > 0.$$

In particular the integral formulas become

$$c_m = \frac{1}{2\pi} \int_0^{2\pi} f(x) e^{imx}\, dx$$

for any m from $-\infty$ to ∞.

The *Discrete Fourier Transform* comes from the left-hand-sum approximations to these integrals. For N equal subdivisions the approximation to the c_m integral is

$$\frac{1}{N} \sum_{k=0}^{N-1} f(k\frac{2\pi}{N}) e^{imk\frac{2\pi}{N}}$$

(we take $x = 0, \frac{2\pi}{N}, 2\frac{2\pi}{N}, 3\frac{2\pi}{N}$... multiply the value of the integrand by $\frac{2\pi}{N}$, and sum). This operation only looks at the N values $f(0), f(\frac{2\pi}{N}), ...f((N-1)\frac{2\pi}{N})$; so given any N-vector $(f_0, ..., f_{N-1})$ we define its Discrete Fourier Transform to be the vector $(c_0, ..., c_{N-1})$ given by

$$c_m = \frac{1}{N}\sum_{k=0}^{N-1} f_k e^{imk\frac{2\pi}{N}} = \frac{1}{N}\sum_{k=0}^{N-1} f_k(\omega^m)^k$$

where $\omega = e^{i\frac{2\pi}{N}}$, a primitive Nth root of 1 (Definition 9.4).

The *Fast Fourier Transform* requires specializing to $N = 2^n$, and putting together several pieces of information.

- We can interpret $\sum_{k=0}^{N-1} f_k(\omega^m)^k$ as the value at ω^m of the polynomial $p_f(x) = f_0 + f_1x + \cdots + f_{N-1}x^{N-1}$ and consequently, by the Remainder Theorem, as the remainder when $p_f(x)$ is divided by $(x - \omega^m)$.
- In any ring, if $a = bc$ the remainder r of p when divided by c can be calculated from the remainder r' of p when divided by a: r is exactly the remainder of r' when divided by c. (Because $p = aq' + r'$ and $r' = cq + r$ give $p = bcq' + r' = bcq' + cq + r = c(bq' + q) + r$; also $r < c$ is automatic. (This is Proposition 9.14)
- $(x^{2^n} - 1) = (x^{2^{n-1}} - 1)(x^{2^{n-1}} + 1)$. The first factor splits again in the same way. For the second, we note that, since ω is a primitive 2^n-th root of 1, we have $\omega^{2^{n-1}} = -1$, so $(x^{2^{n-1}} + 1) = (x^{2^{n-1}} - \omega^{2^{n-1}})$, again a difference of squares, and the splitting can continue. In general $(x^{2^k} + \omega^{2^k})$ may be rewritten as $(x^{2^k} - \omega^{2^k}\omega^{2^{n-1}}) = (x^{2^k} - \omega^{2^k + 2^{n-1}})$. If $k \leq n-1$ then $\omega^{2^k + 2^{n-1}} = \omega^{2^k(1+2^{n-1-k})}$, and the factoring can be repeated. For example $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. Here $\omega = e^{\frac{i\pi}{4}}$ and $\omega^4 = -1$. So $x^4 + 1 = x^4 - \omega^4 = (x^2 - \omega^2)(x^2 + \omega^2)$. As above, $(x^2 + \omega^2) = (x^2 - \omega^6) = (x - \omega^3)(x + \omega^3) = (x - \omega^3)(x - \omega^7)$.
- Last but not least. When $a_0 + a_1x + \cdots a_{n-1}x^{n-1} + a_nx^n + \cdots a_{2n-1}x^{2n-1}$ is divided by $(x^n - c)$ the remainder is $a_0 + a_1x + \cdots a_{n-1}x^{n-1} + c(a_n + a_{n+1}x + \cdots a_{2n-1}x^{n-1}) = (a_0 + ca_n) + (a_1 + ca_{n+1})x + \cdots (a_{n-1} + ca_{2n-1})x^{n-1}$. (Proposition 9.16)

Understand all the steps in this calculation:

f_7x^7		$(f_3+f_7)x^3$		$(f_1+f_5+f_3+f_7)x$		$(f_0+f_4+f_2+f_6)+(f_1+f_5+f_3+f_7) = 8c_0$
$+f_6x^6$		$+(f_2+f_6)x^2$		$+(f_0+f_2+f_4+f_6)$		$(f_0+f_4+f_2+f_6)-(f_1+f_5+f_3+f_7) = 8c_4$
$+f_5x^5$		$+(f_1+f_5)x$		$(f_1+f_5-f_3-f_7)x$		$(f_0+f_4-f_2-f_6)+i(f_1+f_5-f_3-f_7) = 8c_2$
$+f_4x^4$		$+(f_0+f_4)$		$+(f_0+f_4-f_2-f_6)$		$(f_0+f_4-f_2-f_6)-i(f_1+f_5-f_3-f_7) = 8c_6$
$+f_3x^4$	$\to$	$(f_3-f_7)x^3$	$\to$	$(f_1-f_5+i(f_3-f_7)$	$\to$	$(f_0-f_4+i(f_2-f_6)+\omega(f_1-f_5+i(f_3-f_7)) = 8c_1$
$+f_2x^2$		$+(f_2-f_6)x^2$		$+(f_0-f_4)+i(f_2-f_6)$		$(f_0-f_4+i(f_2-f_6)-\omega(f_1-f_5+i(f_3-f_7)) = 8c_5$
$+f_1x^1$		$+(f_1-f_5)x$		$(f_1-f_5)-i(f_3-f_7)$		$(f_0-f_4-i(f_2-f_6)+i\omega(f_1-f_5-i(f_3-f_7)) = 8c_3$
$+f_0$		$+(f_0-f_4)$		$+(f_0-f_4)-i(f_2-f_6)$		$(f_0-f_4-i(f_2-f_6)-i\omega(f_1-f_5-i(f_3-f_7)) = 8c_7$

First arrow: remainder after division by (RADB) $(x^4 - 1)$ (top), RABD $(x^4 + 1)$ (bottom).
Second arrow: from top to bottom, RADB $(x^2 - 1), (x^2 + 1), (x^2 - i), (x^2 + i)$.
Third arrow: from top to bottom, RADB $(x-1), (x+1), (x-i), (x+i), (x-\omega), (x+\omega), (x-i\omega), (x+i\omega)$.
[=RADB $(x-\omega^0), (x-\omega^4), (x-\omega^2), (x-\omega^6), (x-\omega^1), (x-\omega^5), (x-\omega^3), (x-\omega^7)$.]

9.4 In matrix form, the Discrete Fourier Transform is

$$\mathbf{c} = \frac{1}{N}\Omega\mathbf{f}$$

where $\mathbf{c} = (c_0, c_1, \ldots, c_{N-1})$ is the transform of $\mathbf{f} = (f_0, f_1, \ldots, f_{N-1})$ and $\Omega_{j,k} = \omega^{jk}, 0 \leq j,k \leq N-1$ with $\omega = e^{\frac{2\pi i}{N}}$. Understand why Ω is invertible; in fact if the matrix A is defined by $A_{j,k} = \omega^{-jk}$ then $A\Omega = \Omega A = N \cdot I$, N times the identity matrix. So if

$$\mathbf{c} = \frac{1}{N}\Omega\mathbf{f}$$

then

$$\mathbf{f} = A\mathbf{c}.$$

Be able to calculate $\mathbf{f}$ from $\mathbf{c}$ by hand for small values of N.